



Methodology · 6 weeks · \$28,500

CMMC Level 2 Readiness Assessment

All 110 NIST SP 800-171 requirements assessed across your AWS and AWS GovCloud (US) environment, producing the scoping memo, gap analysis, SSP outline, POA&M, and remediation roadmap a C3PAO expects to see.

DURATION

6 weeks

REQUIREMENTS

110 assessed

ENVIRONMENTS

AWS + GovCloud (US)

INVESTMENT

\$28,500

Engagement phases

PHASE	TIMING	WHAT HAPPENS
Scoping	Week 1	Define the CUI boundary: which systems store, process, or transmit CUI, and which are security protection assets. This decision moves assessment cost more than any other, so it is documented and agreed before work proceeds.
Evidence collection	Weeks 1-2	Read-only access through a scoped IAM role, plus collection of existing policies, procedures, prior self-assessment scores, and SPRS submissions.
Control assessment	Weeks 2-4	All 110 requirements evaluated against both the AWS environment and organizational practice. Each is scored met, partially met, or not met, with the evidence reviewed and the gap recorded.
Artifact development	Weeks 4-5	System Security Plan outline and POA&M built from the assessed state, structured the way an assessor reads them.
Delivery and readout	Week 6	Findings walked through with your team, followed by the written package and an executive readout for funding decisions.

Scope of review

AWS SERVICE OR AREA	WHAT IS EXAMINED
AWS GovCloud (US)	Regions supporting DoD Cloud Computing SRG Impact Levels 2, 4, and 5, plus ITAR and FIPS 140-2 validated endpoints
AWS Audit Manager	Evidence collection and control mapping against the NIST SP 800-171 framework
AWS Security Hub, AWS Config	Continuous control monitoring, enabled standards, and configuration drift
AWS CloudTrail, Amazon Security Lake	Audit record generation, retention, protection, and review (3.3.x family)
AWS IAM, IAM Identity Center	Access control, least privilege, separation of duties, and identification and authentication (3.1.x, 3.5.x)
AWS KMS, AWS Artifact	FIPS-validated cryptography for CUI, and inherited compliance evidence from AWS

What we need from you

- Current System Security Plan and POA&M, if any exist
- Prior self-assessment score and SPRS submission date
- Network and data flow diagrams showing where CUI resides
- Policies covering access control, incident response, media protection, and personnel security
- A scoped read-only IAM role for in-scope AWS accounts
- Access to two to four subject matter experts for interviews across IT, security, HR, and facilities

Deliverables

- Environment scoping memo defining the CUI boundary and asset categories
- Control-by-control gap analysis across all 110 requirements, scored with evidence notes
- System Security Plan outline aligned to the assessment objectives
- POA&M with owners, target dates, and effort estimates
- Remediation roadmap sequenced by assessment risk rather than by effort
- Executive readout summarizing posture, cost to close, and timeline to assessment readiness

Assumptions and exclusions

- This is a readiness assessment. Certification must be performed by an authorized C3PAO
- Remediation implementation is quoted separately
- No penetration testing or vulnerability exploitation is performed
- Assessment reflects the environment as observed during the engagement window

Support and service levels

Pre-purchase. Scoping conversations, AWS prerequisite confirmation, and a written statement of work before any private offer is issued. Inquiries answered within two business days.

During the engagement. A named engagement lead, Brian Govanlu, CISSP, as single point of contact. Support Monday to Friday, 9:00 AM to 6:00 PM US Eastern, by email and phone, with a response within one business day. Kickoff within five business days of offer acceptance, weekly written status updates, and a walkthrough of every deliverable.

After delivery. Thirty days of email support for questions about findings and recommendations. Refunds and disputes are handled directly with the engagement lead in accordance with the accepted private offer.

Available directly or through AWS Marketplace as a private offer. If you hold committed AWS spend, the engagement draws down against it and appears on your existing AWS bill. Any AWS infrastructure costs you incur remain your responsibility and are separate from the AWS Marketplace transaction.